Sistematización de experiencia en la compañía de financiación Tuya S.A.

Autor(es)

Angie Carolina García Loaiza

Trabajo de grado presentado para optar por el título de Administrador de Empresas

Asesor

Carolina Herrera Cano

Universidad Autónoma Latinoamericana (UNAULA)

Facultad de Administración

Administración de Empresas

Medellín, Antioquia, Colombia

2023

Tabla de contenido

Resumen:

El presente ejercicio tiene como finalidad sistematizar en detalle las experiencias de la aprendiz profesional en la Compañía de Financiamiento Tuya S.A, en calidad de practicante profesional en el área de Seguridad de la información, en el semestre 2022-2. Tuya es una organización que busca por medio de su operación, una financiación responsable del consumo y fomento de la inclusión financiera como una forma de aportar al desarrollo económico, permitiendo una ampliación del sector crediticio por medio de las diferentes alianzas con las que cuenta la compañía.

El trabajo de sistematización de experiencia se llevó a cabo por medio de diferentes procesos para su construcción, en los que se encuentra la contextualización y caracterización de la organización, el marco teórico y conceptual en relación a las prácticas o terminología existente en el área, las acciones realizadas por la practicante, las reflexiones con relación a las actividades que realizó, enmarcando las enseñanzas, retos, oportunidades, fortalezas y debilidades identificadas en la ejecución de las responsabilidades. Finalmente, se presentan las recomendaciones en el marco de la práctica y los procesos estratégicos y operativo donde se le recomendó a la organización diferentes propuestas para las mejoras en su funcionamiento para disminuir reprocesos y falencias en la ejecución y planeación de las diferentes actividades realizadas por la compañía y el COE de seguridad de la información.

Palabras claves:

Seguridad, sector crediticio, compañía de financiamiento, inclusión financiera, cultura, información.

1. Introducción.

1.1 Características de la organización

Tuya es una compañía de financiación que ofrece créditos y beneficios crediticios a empresas que operan en Colombia como Éxito, Carulla, Alkosto, Viva Air, Claro, Super mayorista, Puntos Colombia, CrediCompra. Tuya S.A. se constituyó bajo el dominio COLOMBO MEXICANA DE INVERSIONES S.A. – COLMEX; luego fue adquirida por el Grupo Suramericana, para convertirse en COMPAÑÍA SURAMERICANA DE FINANCIAMIENTO COMERCIAL S.A. (SUFINANCIAMIENTO); esta empresa estaba orientada a satisfacer las necesidades de crédito de las pequeñas y medianas empresas en el mercado colombiano, créditos a personas naturales con tarjetas de crédito de marca privada, créditos de vehículo y libre inversión, lo que permitía su permanencia en el mercado de crédito de consumo. Posteriormente, fue adquirida por el Grupo Bancolombia S.A. (Tuya, 2022a) y en el año 2015, por el Grupo Éxito con una de las cifras más representativas del sector y permitiendo al Éxito incursionar en mercado financiero con su marca propia de tarjetas de crédito en las que se encuentra tarjeta premium y la cotidiana, la cuales se encuentran según los gustos y necesidades de los clientes (Arteaga, 2015).

A partir del año 2015 la compañía de financiamiento Tuya S.A se ha propuesto innovar el sector financiero y de tarjetas, con el lanzamiento de MasterCard Éxito y Carulla, logrando generar a lo largo de su trayectoria en el mercado nuevas alianzas con otras marcas y crear CrediCompra y Alkosto MasterCard. En el año 2020 se crea una billetera digital de la marca propia Tuya Pay y un canal digital para la venta de tarjetas físicas y digitales. Actualmente, Tuya se encuentra en el proceso de creación de una tarjeta de crédito para Claro, siendo este su nuevo aliado en el mercado.

Así pues, en la actualidad Tuya cuenta con productos relacionados con sus diferentes aliados en los que se encuentra el Éxito en donde se tienen productos como tarjetas marca privada, MasterCard Gold, MasterCard PRO, MasterCard adicional y Tarjeta digital; en tarjetas Carulla con productos de la referencia MasterCard Gold y Black y en tarjetas Alkosto con Alkosto Marca Privada y Alkosto MasterCard (Tuya, 2022a).

En cuanto a su composición accionaria, la compañía de financiamiento Tuya S.A. Cuenta con accionistas como Bancolombia S.A. (24,29%), Banco de Inversión Bancolombia S.A. (25,68%), Pasarela Colombia S.A. (0,017%), Almacenes Éxito

S.A.S. (49,99%) y Almacenes Éxito inversiones S.A.S. (0,096%). Además de lo anterior, al ser estipulada como una compañía de financiamiento, Tuya S.A se encuentra regulada por diferentes entidades como la Superintendencia Financiera de Colombia, Bancolombia S.A., el Fondo de Empleados del Grupo Bancolombia - FEBANC y la Fundación Bancolombia (Tuya, 2021); lo que ha permitido generar alianzas con diferentes empresas y un mayor posicionamiento en el sector crediticio y ampliación de su portafolio de productos.

Esta organización ha buscado posicionarse en el mercado a través de los años, por ello, ha generado a sus clientes servicio y bienestar, proporcionando una financiación responsable del consumo y fomento de la inclusión financiera como una forma de aportar al desarrollo económico del país. Por tanto, Tuya busca ser la puerta de entrada al sector crediticio para más de 1.2 millones de colombianos, convirtiéndose el mejor aliado financiero a través del Banking As A Service o un habilitador que combina las capacidades y experiencias de la compañía al servicio de sus aliados, entregando soluciones financieras y así, generar rentabilidad y sostenibilidad para la transformación de la propuesta de valor de aliados, clientes y empleados (Tuya, 2022b).

De igual manera, la compañía de financiamiento Tuya S.A cuenta con un mapa estratégico como se observa en la figura (1) en donde se encuentra los centros de experiencia los cuales generan la razón de ser de la compañía y el cumplimiento de los objetivos, las estrategias de la organización relacionadas a la evolución digital, la profundización y el fortalecimiento de las soluciones de pago, la diversificación de ingresos y los aliados, dando como resultado una centralización en la experiencia, promoviendo la principal aspiración de Tuya, la cual es ¡soñar con dar oportunidades que transforman vidas positivamente!.

Figura 1
Mapa estratégico

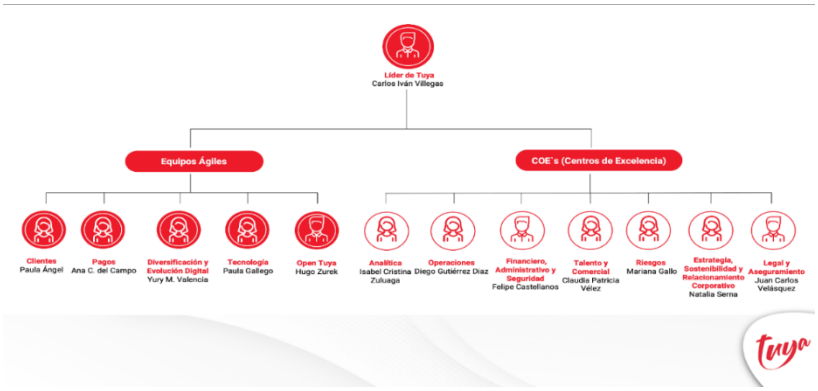
Fuente: Tuya S.A. (s.f.).

De igual forma, en Tuya S.A. Dentro de sus propósitos como compañía se busca generar beneficios a la sociedad, hacerlo posible bajo los valores corporativos como la integridad, flexibilidad, innovación, autonomía, consciencia, el trabajo digno, la equidad, la inclusión financiera y digital. Por ello, la organización está en la búsqueda de valores y fomentación del equipo de trabajo, buscando en ellos una sensibilidad por el cliente, proactividad e innovación; brindando a los miembros de la organización oportunidades de aprendizaje, crecimiento y bienestar en las que se encuentra las comunidades de práctica (tecnología, analítica, experiencia y agilismo) y los beneficios extralegales, económicos y emocionales para mantener la calidad de vida y el balance entre la vida laboral y personal, en donde se encuentra descuentos con los diferentes aliados, privilegios, créditos y tarjetas, fondos de empleados y beneficios de tiempo para compartir con la familia, amigos o eventos especiales (Tuya, 2022b).

En relación con la composición de la organización, esta compañía cuenta con una estructura organizacional horizontal, como se observa en la figura (2), la cual está encabezada por el líder de Tuya (Carlos Iván Villegas) y se divide en dos ramificaciones organizadas entre 1) Equipos ágiles compuestos por clientes, pagos, diversificación y evolución digital, tecnología y open tuya, y 2) centros de excelencia (COE's) en las que se encuentra analítica, operaciones, financiero, administrativo y seguridad, riesgos, estrategia, sostenibilidad y relacionamiento corporativo y legal & aseguramiento (Tuya, 2022a). Estos equipos se encuentran diversificados con el fin de abordar las diferentes perspectivas u objetivos del COE. Así mismo, dicha compañía cuenta con una junta directiva la cual se reúne de manera constante para observar los resultados de los equipos y evaluar acciones a futuro.

Figura 2

Estructura organizacional de Tuya S.A.



- **Fuente:** Tuya (2022). Estructura organizacional de Tuya S.A. https://www.tuya.com.co/nuestra-compania

Por otra parte, Tuya en su proceso para establecerse en el sector de créditos en Colombia ha diseñado y lanzado al mercado nuevas alternativas como una tarjeta de crédito llamada Surtimayorista para contribuir a la reactivación económica y abrir nuevas puertas a las necesidades de comerciantes para la accesibilidad a beneficios y descuentos. Además, esta tarjeta sirve para proporcionar liquidez cuando se requiera de una manera rápida y sencilla. Dicha estrategia es el resultado de la unión entre la compañía y la Surtimayorista para más de 20 tiendas en Bogotá, Barranquilla y Villavicencio, generando beneficios en cuanto a la realización de retiros y pagos de los costos asociados al uso de la tarjeta en las empresas aliadas a Tuya S.A. (Analitik, 2022).

En cuanto al crecimiento de Tuya en el sector crediticio, según lo mencionado por La República (2022), actualmente el país cuenta con más de 16 millones de tarjetas de crédito y débito vigentes en el país, de las cuales según el reporte emitido por la Superintendencia Financiera de Colombia, la compañía de financiamiento Tuya S.A se ha posicionado como la entidad líder de tarjetas de crédito, lo cual se evidencia en la figura (3), contando con más de 2.446 millones tarjetas, seguida de Bancolombia con 2.441 millones y de Scotiabank Colpatria con 2.3 millones de tarjetas, teniendo presente que en el valor total de las tarjetas se encuentran las canceladas y vigentes. Además, con la participación de Tuya en las copias con MasterCard, ha logrado que sea la primera empresa impresora con un aproximado de 6,8 millones de copias, seguida de visa con 5,7 millones (Vesga, 2022).

Figura 3

Reporte emitido por la Superintendencia Financiera de Colombia.

REPORTE TARJETAS DE CRÉDITO

Entidad	Vigentes a la fecha de corte	Vigentes durante el mes	Canceladas
Tuya	2.446.341	55.486	84.952
Bancolombia	2.441.258	94.353	66.582
Scotiabank Colpatria S.A.	2.309.830	51.776	31.604
Banco Falabella S.A.	2.199.427	45.586	31.515
Banco Davivienda	1.343.530	41.963	24.449
Banco de Bogotá	1.258.593	48.554	29.176
Banco Serfinanza S.A.	779.021	18.821	6.736
BBVA Colombia	778.762	32.348	18.046
Banco de Occidente	557.526	9.502	6.885
AV Villas	498.668	8.512	5.720

- **Fuente:** La República (2022). Reporte de tarjetas de crédito. https://www.larepublica.co/finanzas/los-lideres-en-tarjetas-de-credito-vigentes-se-mantienen-siendo-tuya-y-bancolombia-3432529

No obstante, al pertenecer al sector crediticio y evidenciando distintos comportamientos económicos y financieros que ha tenido Colombia en los últimos tiempos, según un artículo de la revista Semana se cuenta que Tuya, Falabella y Banco de Bogotá están liderando el ranking con más tarjetas de crédito bloqueadas en 2022, es decir, a pesar de ser una de las entidades bancarias con más tarjetas de crédito vigentes, Tuya se encuentra en el segundo lugar con un total de 255.895 plásticos bloqueados, lo que puede ocasionar un riesgo existente por los cambios que esto puede producir en el futuro financiero del país y las afectación al progreso de Tuya como compañía de financiación. Además de esto, también genera la preocupación por la demanda para la adquisición de este servicio y sus repercusiones para posibles ampliaciones en su portafolio de productos (Semana, 2022).

Además de lo anterior, Tuya al incrementar de popularidad en el sector en que opera y sus alianzas estratégicas con distintas entidades reconocidas en Colombia, ha recibido diferentes amenazas que ponen en riesgo su seguridad y la de sus clientes. Esto se debe a que han existido diferentes denuncias ciudadanas sobre un correo aparentemente fraudulento, asociado a la tarjeta de crédito Tuya del grupo Éxito, donde, según parece, cibercriminales estarían enviando enlaces con la excusa de que la cuenta fue bloqueada y el “error” solo se podría solucionar por medio de la URL o enlaces maliciosos que la persona debería entrar y así robar su información o extorsionar a cambio de una cantidad de dinero. Según lo dicho por la compañía, está comprobado que el correo no fue enviado por la compañía Tuya y que acciones como esta corresponden a una modalidad de ciberdelincuencia (phishing), con la que personas malintencionadas obtienen información personal y bancaria de quienes ingresan a los enlaces que son generados y enviados por estos delincuentes (El Colombiano, 2022).

Lo anterior deja en evidencia cómo la compañía de financiación Tuya S.A., además de la búsqueda por incrementar su portafolio de productos y servicios en el mercado nacional por medio de alianzas con distintas empresas, también debe tener presente y monitorear constantemente los comportamientos económicos y financieros existentes en el tiempo y velar por la seguridad y la protección de la información de sus clientes, aliados, proveedores y empleados.

1.2 Funciones centrales de la práctica y otras actividades

En la organización Tuya S.A. me encuentro como practicante del equipo de seguridad de la información correspondiente al COE de Riesgos anteriormente evidenciado en la figura 2. En dicho COE, se tiene como objetivo proteger a los

clientes y generar confianza en los aliados a través de estrategias proactivas e innovadoras, desde la gestión para riesgos financieros y no financieros, habilitando el adecuado balance entre experiencia, sostenibilidad y crecimiento responsable de Tuya S.A. Además, el COE se enfoca en la realización de las definiciones de políticas, lineamientos y objetivos específicos relacionadas con el riesgo de información y de seguridad de la organización, así como la definición e implementación de los componentes del sistema. Este sistema se compone de la identificación, evaluación, medición, administración, monitoreo, control y reporte de los riesgos. Adicionalmente a esto, en el COE de Riesgos se crea y se hace seguimiento de un mapa de riesgos, identificando los límites mínimos y máximos de exposición (apetito de riesgo), factores para tener en cuenta, etc. (Tuya, 2022).

En este conjunto llamado COE de riesgos, existen subconjuntos de riesgos no financieros pertenecientes a SMT, COEs y equipos de trabajo, en los que se encuentra: Infraseg, Control de Accesos, Cyber Ops, Seguridad del Negocio y Seguridad de la Información. No obstante, en este caso en particular se hablará del COE de Seguridad de la Información, el cual por medio de sus estrategias busca generar una cultura y filosofía encaminadas al principio de autocontrol y generación de acciones conscientes frente a las responsabilidades y toma de decisiones de los miembros de la organización ante posibles amenazas cibernéticas que puedan afectar o poner en riesgo la seguridad de la información de aliados, clientes y colaboradores y a su vez, la sostenibilidad de la organización (Palacio, 2021).

Teniendo en cuenta lo anterior, durante el periodo de prácticas profesionales en el COE de seguridad de la información, se realizaron funciones como actividades, ejercicios en torno a la cultura de la organización, inventario de activos, recopilación de información, apoyo al monitoreo del presupuesto del equipo y entre otras actividades que se profundizará en el desarrollo del trabajo.

2. Contextualización

2.1 Contextualización del proceso organizacional

El COE de Seguridad de la Información, tiene en cuenta las estrategias que componen las actividades y lineamiento de este equipo, en las que se encuentran: las corporativas, análisis de riesgos estratégicos y operativos, la normatividad y la buena práctica. Estas funciones permiten definir y actualizar las actividades, programas y planes de acción relacionados con el área para generar una seguridad definida en la recopilación y almacenamiento de evidencias relacionadas con el cumplimiento y buen manejo del ejercicio; por tanto, el centro de excelencia realiza entre sus tareas más destacadas, programas de cultura en la cual se define y

ejecuta actividades relacionadas con la concientización, realizando seguimientos para la efectividad y las evidencias de la campaña por medio de actividades, simulacros o campañas de seguridad. Asimismo, se tienen en cuenta los lineamientos relacionados con iniciativas y necesidades de la compañía y la presencia de requisitos legales y regulatorios (Palacio, 2021).

Ahora bien, como parte de las estrategias ya mencionadas, el equipo cuenta con diferentes políticas, ejercicios, simulacros, sesiones y actividades enfocadas en formar las buenas prácticas de seguridad, para lograr a nivel empresa una categorización del empleado, según su formación en temas relacionados con la conciencia, protección y prevención de riesgos con la información; para ello, se utilizan dos tipos de términos de manera interna como 1) Ninja haciendo referencia a las personas que piensan, paran y actúan ante una amenazas y cuentan con el conocimiento y conciencia necesaria para prevenir los riesgos cibernéticos o fugas de información y 2) Marrano como aquel sujeto que, de manera mecánica, no tiene en cuenta las alertas de seguridad y atiende sin algún tipo de protección o conocimiento de actos sospechosos producidos o generados por cibercriminales provocando fuga de información, infiltración en el sistema, robo o soborno en relación a la información, afectando la seguridad e integridad no solo de la compañía sino también de todos aquellos que la componen, incluyendo clientes, aliados y empleados.

Dentro del proceso de la organización, el cumplimiento de las actividades propuestas y el fomento de buenas prácticas con respecto a la seguridad de la información y la organización en sí, el COE realiza ejercicios de seguridad existentes en diversas modalidades actualizándose de manera constante según la evolución de ataque de los cibercriminales. En primer lugar, está la modalidad de ataque a través del *Phishing*, es decir, un ataque generado al abrir enlaces maliciosos o archivos adjuntos de correo electrónico disfrazados de algo interesante (Belcic. 2020), también está el *Smishing*, que se refiere a una modalidad de ataque, a través de mensajes de texto o de WhatsApp se envían enlaces maliciosos con el fin de engañar a los clientes y obtener su información. Por último, está el *Vishing* que es un tipo de amenaza que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet para robar información y dinero a las víctimas (Ventura, 2021). Además, está el BEC (Business Email Compromise) que hace referencia a correos maliciosos enviados internamente desde la compañía, ya sea por plagio o robo de información y en general.

Se debe tener en cuenta que las amenazas o ataques generados a través de Phishing, Vishing, Smishing, BEC, etc., son utilizados con el objetivo de robar información, dinero e identidades a través de la manipulación de las emociones a

las víctimas, implementando esto como la principal herramienta y la puerta de entrada a las organizaciones o personas. Por esta razón, Tuya se enfoca en prevenir estos ataques a través de diferentes modalidades de simulacros y ejercicios para generar una conciencia responsable a los equipos de trabajo y así, evitar este tipo de incidentes.

Además de lo anterior, dentro de las actividades del COE de Seguridad de la Información, se realiza la elaboración y control del inventario de activos de información con el fin de realizar la consulta y recopilación de información de los diferentes equipos se encuentran en la compañía para la identificación del manejo, utilización, recopilación y almacenamiento de información confidencial y prioritaria de los clientes, empleados o tarjetas, ya sea en aplicativos, carpetas de red, correos electrónicos, etc.. Además, este equipo realiza la verificación y el manejo asertivo de la Virtual Private Network (VPN) ya sea básica o por TWA, evitando filtraciones de red y haciendo controles para el manejo adecuado de esta.

Así mismo, se realiza los Indicadores del Instituto Nacional de Estándares y Tecnología (NIST) para la gestión de riesgos asociados a la seguridad de la información y la identificación del nivel de madurez a nivel compañía y equipos de trabajo, el presupuesto del área y modelado de roles en donde se identifica y evalúa las limitación o accesos de las funciones y permisos que tienen los miembros de la empresa según su rol administrativo o técnico, para ello, se utiliza el principio de mínimo privilegio y los frentes de trabajo desde el cual se gestione.

Las actividades y ejercicios anteriormente mencionados son realizados hace aproximadamente 8 años, debido a que, la organización a través de la búsqueda de alternativas y soluciones para la prevención de la fuga de información y control de la seguridad en relación a la información como el activo primario de la compañía, identificó la necesidad de buscar herramientas y estrategias para fomentar una cultura para protección de la información; de ahí, nacen los ejercicios de Phishing, BEC y semejantes. Además de esto, se vio la necesidad de identificar la información de cada una de las áreas, analizando los permisos de aplicativos y utilidades, la protección de la red de la organización e indicadores que permitan medir el riesgo y la seguridad con el fin de disminuir la posibilidad de fuga de datos o acciones criminales que puedan comprometer la reputación y operatividad de la organización.

No obstante, a pesar de ser un beneficio para Tuya en cuestión de protección, esto ha significado un desafío para el COE de Riesgos en general y los equipos que contribuyen a la seguridad ya sea física o no, debido al descuido de las personas que proporcionan información descartando las políticas y reglamentos de seguridad afectando de manera directa la integridad y reputación de la organización. Además

de lo anterior, se identificó como limitante la pandemia de 2019, que afectó no solo la seguridad y la ampliación de las vulnerabilidades de la compañía, sino también, por cuestiones de accesos, se generó una ampliación de los privilegios en cuestión de aplicativos, dando como resultado un riesgo mayor en cuestión de infiltración o robo de información.

Teniendo en cuenta las actividades realizadas en el COE, como practicante he desempeñado diversas funciones como: la participación en el monitoreo del presupuesto del área; la recopilación, seguimiento, citación y control de las actividades de cultura de la seguridad; acompañamiento en los ejercicios de BEC, Phishing y semejantes. Asimismo, realizó el inventario de activos con los líderes de las áreas sobre el dominio de información, almacenamiento y distribución de la información en los aplicativos o herramientas usadas para esto, participó en las pruebas de seguridad que se realizan de manera cíclica en las dos plantas, enviando los consolidados de madurez y apetito de riesgos de acuerdo con los ejercicios realizados, los resultados objetivos y el indicador NIST.

2.2 Contextualización teórica y/o conceptual del proceso

Para la realización del ejercicio de sistematización de experiencia y con el fin de contextualizar sobre las actividades que, como practicante desempeño dentro de la compañía de financiamiento Tuya S.A, presentan algunos conceptos y teorías los cuales dan claridad y encaminan el desarrollo del presente trabajo. En primer lugar, se hace referencia a la a la gestión tecnológica, en la cual se realiza un conjunto de procesos para la identificación, evaluación, adquisición e incorporación a la organización, lo que permite una optimización y mejora continua de la tecnología necesaria para la ejecución de los proyectos y enmarcar dentro de estos la innovación como factor fundamental para promover y controlar el cambio tecnológicos dentro una organización como Tuya S.A y el entorno, logrando ventajas competitivas y la permanencia de la empresa en el tiempo (Núñez, 2011).

Aunque la tecnología permite a la organización tener una mayor productividad y acceso a información, también conlleva una responsabilidad con respecto a los problemas de seguridad que se puedan generar por ella. Es por ello que, el término de la seguridad de la información se considera un concepto fundamental para el desarrollo del trabajo, este se podría definir como aquel proceso o metodologías que buscan proteger la información y los sistemas ya se por el acceso, uso, divulgación, modificación o destrucción de la misma, es decir una protección a los datos y los recursos de infraestructura tecnológica que cuentan organizaciones como Tuya (Vega, 2021).

En tuya se considera la información como el activo más importante y por ello, se realizan actividades y ejercicios para la preservación de la misma. en este caso, se hablará del inventario de activos de información no físicos, que según la Agencia Nacional de Defensa Jurídica del Estado (2016) es la “información que se recibe o produce en el ejercicio e incluye información que se encuentre escrita, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos” (pág.3); es decir, aquella información que maneje, transmita o ejecute por cada uno de los equipos pertenecientes a Tuya incluyendo el uso de aplicativos, carpetas compartidas, correos con información entrantes o salientes a terceros o equipos de trabajo, clasificando dicha información en niveles según la confidencialidad, la criticidad y susceptibilidad que dicha información presente.

Además de lo anterior, se realizan los simulacros de Phishing, Smishing, Vishing y BEC, los cuales han sido definidos anteriormente y que hacen parte de la cultura de la seguridad. Sin embargo, al realizarlos a manera de simulacros dentro de la organización Tuya S.A, permite disminuir la posibilidad de que, un ataque real se filtre, acceda o afecte la funcionalidad de la empresa por causa de cibercriminales, debido a que, Según lo mencionado por Ventura, (2021) el Phishing, Smishing y Vishing son los fraudes electrónicos como llamadas, correos electrónicos y mensajes, siendo estos los más usados por los ciberdelincuentes para robar datos privados, pero se puede evitar sus daños, utilizando como principal herramienta el sentido común y la prevención antes de compartir información “Ante la duda, me abstengo” (Ventura, 2021).

De igual forma, el BEC al ser correos con personas internas de la organización, tienen mayor posibilidad de ocurrir, debido a que son diseñados estudiando la empresa a detalle e identificando un punto débil, es decir, utilizando la ingeniería social o el acceso a la información para comprometer las cuentas de los correos electrónicos corporativos utilizando como principales herramientas la manipulación de emociones y la suplantación; no obstante, estos pueden ser evitados bloqueando correos sospechosos, habilitando el factor de doble autenticación y atendiendo capacitaciones para entender y prevenir dichos ataques (Centro Cibernético Policial, s.f).

Con los resultados obtenidos en los simulacros de Phishing, Vishing, Smishing y BEC, se realiza una medición para identificar el nivel de madurez y el apetito de riesgo de la compañía de financiación Tuya S.A; el primer término según Mera, Baque & Soler (2019) se podría definir como una escala para medir las capacidades para mantener desarrollar y seguir creciendo en la gestión de los activos manejados, considerando un conjunto de objetivos que caracterizan y estabilizan la

organización. Así mismo, al apetito de riesgo es el nivel de riesgo que la empresa está dispuesta a aceptar y tolerar en consecuencia del cumplimiento o meta de sus objetivos y, además, permite la toma de decisiones, y el seguimiento y monitoreo de los resultados obtenidos y los riesgos asociados a este (La FPIAE,2013).

Dentro de las actividades realizadas dentro de cultura de la seguridad, se realiza la recopilación de información para temas de cultura de la seguridad. La recolección de información se puede definir como un proceso de manera coherente para obtener información o resultados que contribuyan al logro del objetivo, obteniendo variables que intervienen de manera directa o indirecta en el proceso (Gallardo & Moreno, 1999), en el caso de cultura de la seguridad, se realiza la recopilación de información sobre usuarios, actividades o ejercicios que puedan ayudar o identificar mejoras en cuanto a la concientización y evaluación del impacto y trayectoria de la seguridad en cada miembro de la organización. Dicha información se almacena en un Instrumento tipo EDT para la realización de reportes, promedios o número de asistencias.

De igual forma, se tiene el apoyo al monitoreo del presupuesto, el cual ha sido definido por Ramírez (s.f) como “la determinación y asignación de los recursos requeridos para la consecución de los objetivos” para lograr de manera eficaz la empresa o el área a mediano o corto plazo, siendo en este caso una hoja de trabajo FORECAST para programar el uso o ahorro del efectivo para futuras actividades o planes que se quieran lograr en el equipo de seguridad de la información como campañas de cultura, semana de la seguridad, etc. Dicho presupuesto se realiza anualmente, pero se revisa mensualmente para identificar nuevos gastos, ahorros o mayor inversión en actividades según su nivel de impacto y la capacidad adquisitiva que se tenga.

Finalmente, se menciona el Marco de Ciberseguridad del NIST el cual sirve para comprender a manera de detalle los riesgos de ciberseguridad y cómo administrar y reducir los riesgos generados en este. Además, permite la protección de los datos y la información de la organización (NIST, s.f). En Tuya, se incorpora este marco por medio de los cinco pasos como la identificación, protección, detección, respuesta y recuperación, siendo integradas por los medidores correspondiente para su efectivo funcionamiento de acuerdo con el área y comportamiento. Además, del monitoreo constante y fuente de información para reportes e informes a entidades de control.

3. Ejecución.

Como practicante en el COE de seguridad de la información, con el fin de cumplir las labores asignadas y generar una participación en las estrategias y objetivos del equipo, desde el inicio de la práctica la líder (Claudia Milena Palacio) me designó las actividades relacionadas con cultura de la seguridad, participando en las inducciones y formaciones ya sea a proveedores o reincidentes (personas que, a pesar de las señales entregan su información personal y de la compañía en los ejercicios o simulacros) como primer acercamiento a lo que sería una tarea matutina y en la que se busca como propósito principal contextualizar a los nuevos colaboradores, terceros y colaboradores antiguos, además de los reincidentes que hacen parte de Tuya S.A sobre la contextualización y entendimiento de las amenazas existentes y las herramientas para defenderse ante los ataques, en estas actividades fui acompañada, guiada y asesorada por uno de los analistas de seguridad de la información y expertos en el tema de cultura.

Al tener un mayor entendimiento en relación a los procesos y la actividad que se realizaba en el COE, puede tener mayor colaboración a medida que fuera pasando el tiempo, apoyando en la recolección de la información relacionada con el ejercicio mencionado anteriormente, realizando la citación para las sesiones de fortalecimiento ante amenazas y la comunicación para líderes y personas ya sean empleados o terceros que, por descuido o falta de conocimiento han entregado su información o accedido a enlaces en los simulacros que se realizan mes a mes en sus diferentes modalidades (Phishing, Vishing, Smishing y BEC).

Además de lo anterior, y como estrategia encaminada a la cultura de seguridad de la compañía de financiamiento Tuya S.A, se realizan por parte del área y con el acompañamiento de Forensict y mi persona, diferentes simulacros de manera cíclica con el fin de prevenir amenazas internas o externas a la organización, realizando ejercicios por medio de controles de antivirus, conexiones a la red (inalámbrica o cableado) seguras, los bloqueos de dispositivos de almacenamiento externo, el flujo de datos DLP, cifrado de disco y otros métodos que permiten mitigar el riesgo a posible filtraciones y las amenazas que puedan provocar una alerta de seguridad o en el peor de los caso, un daño a la organización en relación a la operatividad, funcionalidad y reputación.

Con el paso del tiempo y tener más apropiación de los temas del área y movimientos que se realizan en el equipo, me fue asignado junto con el analista de seguridad de la información el presupuesto del área. Para la ejecución de esta tarea, se debe identificar mes a mes los gastos, costos, ahorros y movimientos financieros fijos o variables que se realizaron y consignando en el FORECAST como libro mayor o libro de seguimiento. Posterior a eso, dicho documento es enviado al equipo de financiera encargado de llevar el control del presupuesto a nivel general de la compañía.

Entre las actividades que he realizado durante la práctica se encuentra el inventario de activos de información no física, el cual ha sido realizado como apoyo al analista de seguridad del negocio para lograr los objetivos propuestos en el Q y en el área. Para ello, como inducción a la actividad, se asignaron diferentes espacios con el fin de conocer el instrumento para la toma de información, los pasos para la realización óptima de la tarea y la agenda para citar a los diferentes líderes de las áreas existentes en Tuya y posterior a esto, llenarlo con la información respectiva.

Finalmente, de manera no muy común y cumplimiento con el plan de fortalecimiento de protección ante amenazas, se realizan diferentes talleres y seguimientos sobre alertas de seguridad a los equipos que se encuentran en planta y sesiones virtuales a los diferentes equipos de la organización para hacer claridades sobre el tema, prevenir amenazas y solucionar preguntas o dudas existentes por los asistentes, relacionadas a la seguridad de la información de la organización y a la mitigación de los riesgos existentes relacionados a la infraestructura y nombre (reputación) de Tuya S.A.

Con el fin de especificar a mayor detalle lo mencionado en los párrafos anteriores en relación con las actividades que se realizan en la práctica profesional en el área de seguridad de la información, se presenta la siguiente tabla (1), en donde se muestra el tipo de actividad, el tiempo o periodo de ejecución, las tareas correspondientes y sus respectivas descripciones, dando claridad.

Tabla 1: **Actividades que se realizan en la práctica.**

ACTIVIDAD	TIEMPO	TAREA	DESCRIPCIÓN
Ejercicio BEC	Dos ejercicios por mes	Seguimiento	Se realiza el simulacro de prueba con el correo de suplantación de un líder y posterior a ello, se envía a un número determinado de personas y se monitorea su funcionalidad y reportes a correosospechoso@tuya.com.co. También, se monitorea el tiempo de respuesta ante este tipo de incidentes y los procesos que realizan cada uno de los miembros del equipo, ya sea reportar, llamar al líder o acceder al sitio o enlace enviado.
		Recopilación de datos	Se reúne toda la información obtenida como el número de personas que participaron, reportes a correo sospechoso y los que cayeron en el ejercicio, felicitando y haciendo llamados de atención según sea el caso.
			Al recibir el reporte final de usuarios que participaron se realiza una felicitación o llamados

		Citación de usuarios	de atención según sea el caso a los participantes del ejercicio. Las personas que cayeron en este ejercicio son llamadas para una citación sobre cultura de la seguridad para reforzar las herramientas y evitar incidentes y se agregan en el consolidado de campañas.
Ejercicio Phishing, Vishing y Smishing	dos ejercicios por mes	Diseño	Se realiza reuniones con el proveedor (Csiete) para el diseño del ejercicio teniendo en cuenta la temática, herramientas a usar (correos, mensajes, llamadas o enlaces) y número de usuarios a los que va dirigido, enviando un correo con la información respectiva al proveedor con el dominio, diseño y muestra para la respectiva actividad.
		Simulacro y seguimiento	Luego de la entrega del proveedor, se realiza un simulacro por parte de los miembros del área para confirmar funcionamiento o mejoras al ejercicio. Posterior a esto, se envía por el canal que se eligió y se realiza seguimiento de usuarios.
		Entrega de informe	Pasados 72 horas del envío del ejercicio, el proveedor recolecta la información de la campaña y realiza un informe final del ejercicio, en el cual se evidencia la finalidad del ejercicio, el diseño y el número del ingreso, vistas e información suministrada por las personas que cayeron en el ejercicio para realizar la consolidación con la información y el reporte sobre el índice de madurez a seguridad del negocio.
		Citación a usuarios	Se envía un correo a la compañía en donde se informa del ejercicio y el resultado de este, siendo enviada con la información respectiva a los líderes y personas involucradas. Además, se realiza la citación a las personas que cayeron para una sesión de reincidentes en cultura de la seguridad.
Inventario de activos de información	Según agenda Con meta mínima de 5 por Spring	Citación	Se envía un correo y un mensaje vía Teams a los líderes de las áreas para definir según su disponibilidad una sesión de 30 minutos, teniendo en cuenta la información suministrada en un formulario sobre el dominio o uso de información de tarjetas, empleados o clientes.
			En la sesión se preguntan temas relacionados con la información que almacenan de clientes,

		Entrevista	empleados o tarjetas. Dicha información se recopila en una base de datos con los ítems correspondientes al activo, descripción, datos que almacena, nivel de criticidad y baúl o lugar en que se almacena.
Recopilación de información	Semanal	Búsqueda y organización de información	De acuerdo con las sesiones realizadas por culturas de la seguridad ya sea por reincidentes, inducción a proveedores, inducción empleados o actividades extras sobre seguridad, se realiza la recolección de información como: asistencia, calificación, nombre y cédula del colaborador o tercero. Lo anterior, es almacenado en un instrumento diseñado en Excel para información de interés a la compañía y al COE.
Presupuesto	Mensual	Organización de información	Se realiza un presupuesto según los gastos obtenidos en el periodo y se toman decisiones. Mes a mes se hace envío de un formato llamado FORECAST donde se encuentra la información contable de cada una de las áreas con sus respectivos gastos, movimientos y dinero restante para los próximos meses.
Pruebas de seguridad cíclicas	1 por mes	Planeación	Se realiza junto al proveedor (forensict) un plan de trabajo, donde se encuentra el tipo de ejercicio, modo de ejecución, tiempo de realización y lugar a realizar.
		Ejecución	Se designa un día durante el mes para realizar este ejercicio, realizando 9 diferentes pruebas y mirando su efectividad o control. Para la realización se selecciona un equipo de cómputo al azar de cualquier miembro de la organización en las diferentes oficinas de Torre Tuya y CEOH para realizar las respectivas verificaciones.
		Control	Finalizada la ejecución del ejercicio de pruebas, el proveedor envía un documento donde se evidencia el tipo de prueba, como se practicó y el resultado que se obtuvo. Con los resultados se crea un plan de acción con las diferentes áreas correspondientes y así, evacuar la amenaza, la cual se pondrá en prueba al mes siguiente.

Fuente: elaboración propia basada en las actividades asignadas y realizadas por la practicante del área de Seguridad de la información en el periodo 2022-2.

4. Reflexiones.

4.1 Reflexiones sobre el proceder de la organización a partir del proceso en el que se participó

La compañía de financiación Tuya S.A busca brindar oportunidades para transformar vidas positivamente y para ello, busca un equipo de trabajo que se ajuste a las necesidades y objetivos de la empresa. Por esto, al momento de realizar la selección de alguna vacante se enfatiza en su formación profesional y sus metas u objetivos a nivel personal. A manera personal, el proceso de selección para practicante del COE de seguridad de la información, se realizó una entrevista con la líder del área donde se habló no solo en las capacidades de la aspirante para el cumplimiento de las actividades, sino también, del ámbito personal, utilizando preguntas enfocadas en los objetivos, aspiraciones y conocimiento de la persona, permitiendo así, una facilidad para conocer o entender a la entrevistada y tomar decisiones.

Al ingresar a la organización como administradora de empresas fue un reto el entendimiento y la adaptabilidad, no solo por la complejidad de términos debido a que, esta área está focalizada para ingenieros y especialistas en temas relacionados con los sistemas, telecomunicaciones, ciberseguridad o similares; sino también por la filosofía de trabajo con la que cuenta Tuya S.A. No obstante, al pasar del tiempo, esto significó una ayuda como practicante designada en el área, ya que generó un esfuerzo, permitiéndome salir de la zona de confort, organizarme y prepararme para comprender cada día más los temas de seguridad, información y la compañía en general, buscando estar alineada con el contexto de la seguridad, los manejos de información y el cumplimiento de actividades y objetivos propios del área.

En cuanto a mi adaptabilidad como practicante en el COE de seguridad de la información, ha significado un aprendizaje autónomo y enfocado en los nuevos contextos del trabajo debido a que, al ser un área operativa se debió realizar un estudio constante en cuanto a la terminología, la practicidad y el énfasis que se le da a cada actividad dentro del equipo, lo cual implicó la familiarización en relación con el trabajo en oficina y remoto. Además, esto implicó entender el tema de la seguridad de la información y las normativas, términos y prácticas que en el COE se ejecutan.

Por tanto, dentro de mi práctica profesional en el área de seguridad de la información, pude entender y evidenciar los procesos que se realizan en el día a día y la importancia que esto representa para el cumplimiento de los objetivos, el control y prevención de las amenazas en la organización. Además, dentro de la práctica se identifica el trabajo bajo los pilares de seguridad y sus complementos, entendiendo con ayuda de mis compañeros y de manera autónoma la complejidad de las labores, así como el conocimiento de la metodología de trabajo de la organización por medio del agilismo y la priorización, orden y control de las responsabilidades para así, cumplir los objetivos propuestos.

Desde mi punto de vista, conociendo y entendiendo poco a poco la metodología de trabajo es posible decir que, a pesar de las dificultades al inicio de este proceso debido a la falta de entendimiento en relación con las actividades, estrategias y desarrollo de los ejercicios, este es un equipo que de manera indirecta complementa a todos los equipos de la organización y que de manera interna, cuenta con personas capacitadas y con disposición para acompañar, asesorar, enseñar y ayudar en las diferentes solicitudes que lo requiera y que de manera personal me quedo con grandes enseñanzas y apoyo de parte de ellos.

4.2 Reflexiones teóricas o conceptuales

Las teorías y conceptos abordados en el transcurso del trabajo dan funcionalidad y contexto a las metodologías y ejercicios realizados por el COE de seguridad de la información, los simulacros de seguridad, las cuales se ejecutan siguiendo la teoría expuesta por los diferentes autores y los lineamientos realizados de manera interna por los miembros del equipo, como pauta para la ejecución y los resultados óptimos para los indicadores de madurez y de seguridad que aquí se realizan.

En este sentido, se puede decir que las teorías y conceptos abordados por los diferentes autores como Ventura (2021) en donde se menciona el fraude efectuado por medio del Phishing, Smishing, Vishing; Centro Cibernético Policial (s.f) donde se menciona los peligros que se pueden generar a la organización por medio ataques cibernéticos como el BEC y lo dicho por la agencia nacional de defensa jurídica del estado (2016) para hacer referencia a los inventarios activos para la preservación de la información y las buenas prácticas para minimizar los riesgos. Esto es expuesto en el trabajo como aquellas definiciones que permiten clarificar y entender el fin de la misma y los demás ejercicios o actividades que son realizadas y se aplican en su totalidad dentro del grupo y las estrategias de trabajo, puesto que como área de seguridad de la información las funcionalidades, actividades y ejercicios están enfocadas en la seguridad, el control y manejo asertivo de la

información, y detección anticipada de posibles amenazas que ponen en riesgo la compañía Tuya S.A.

Además de lo anterior, dentro del área de seguridad también se cumple los lineamientos establecidos y mencionados por NIST (s.f) y Mera, Baque & Soler (2019) en relación con el indicador Nist y el nivel de madurez, dando efectividad a los objetivos del equipo y el apetito de riesgo designado por la organización. Así mismo, dentro del cuidado, control y manejo de la información, se encuentran establecidas diversas propuestas como el inventario de activos de información no física y modelado de roles, definida por el principio del mínimo privilegio y la preservación de la información de la compañía.

De igual forma, se tiene en cuenta lo mencionado por Núñez (2011) en donde se aplica la gestión tecnológica para los procesos para la identificación, evaluación, adquisición a la organización Tuya S.A , para la ejecución, optimización y mejora continua de las tecnología necesarias para la ejecución de los diferentes proyectos existentes en la organización y enmarcar dentro de estos la innovación como factor fundamental para promover los cambio tecnológicos dentro una organización para lograr ventajas competitivas. De igual manera, se habla de la seguridad de la información, como concepto que guía y ayuda al mayor entendimiento del trabajo, para ello, se implementa lo mencionado por Vega, (2021), siendo este una metodología para la búsqueda de la protección la información y diferentes sistemas para el cuidado y preservación de activo más valioso de Tuya el cual es la información

Lo anterior da como resultado una sinergia entre la teoría y la práctica, es decir, la funcionalidad del término en relación con la aplicabilidad de estos en las actividades, objetivos y propuestas encaminadas en la prevención de amenazas, cuidado de la infraestructura no física y el manejo de la información, por medio de los simulacros, talleres, ejercicios y lineamientos que el área realiza.

4.3 Reflexiones sobre el proceder del practicante a partir del proceso en el que participó.

El proceso dentro del COE de seguridad en el cargo de practicante ha sido una experiencia gratificante y retadora a nivel personal y profesional. Por un lado, lo gratificante ha sido el aprendizaje autónomo para comprender el área de la práctica y la ciberseguridad. Por otro lado, esta experiencia resultó retadora debido a la complejidad que implica para una administradora comprender modelo operativo del área de seguridad de la información. Para poder realizar este proceso tuve que

apropiarme de la teoría, la cual alimenta el proceso y además, adquirir nuevos conocimientos y realizar un estudio constante de herramientas, tecnologías, estrategias y actividades que permiten al equipo de seguridad ir un paso más adelante del cibercriminal y proteger la información de la compañía de financiación Tuya S.A.

Desde mi llegada me sentí acogida por el equipo y la líder del área. Los primeros contactos fueron realizados de manera virtual y luego una explicación de manera presencial permitiéndome, a pesar de los nervios, interiorizar de manera paulatina la información. Para el entendimiento de estos temas, fue necesario el uso de diapositivas, ejercicios y reuniones sobre la metodología de trabajo, las herramientas de uso cotidiano, las tareas por realizar y la programación de las actividades para su monitoreo y control.

A medida que fue pasando el tiempo, tuve un mayor acercamiento con mis compañeros, dejando a un lado la timidez para así, conocerlos mejor y poder interactuar de manera asertiva con ellos y a su vez aprendiendo y generando experiencias positivas que me han ayudado a mejor en el cumplimiento de mis actividades y mis capacidades de relacionamiento. Así mismo, esto permitió una ampliación en el contacto con personas externas al equipo, facilitando el contacto y solicitud para diferentes procesos que se realizan ya sea encuestas, encuentros, talleres o comunicación de manera específica y personalizada.

No obstante, como administradora de empresas tuve muchas limitantes en cuestión del conocimiento en relación a teoría-práctica, es decir, entender la terminología existente y con ella, realizar los procesos y ejercicios prácticos que reflejan no solo la capacidad de respuesta por medio de ejercicios como el Phishing, Vishing, Smishing o BEC y el medidor de madurez, sino también el control de la organización en cuanto a la información por medio del modelado de roles y el indicador Nist y seguimiento a este por medio del inventario de activos no físicos. Además, dichas limitaciones impidieron en algunas cosas realizar de manera oportuna las actividades solicitadas por el equipo.

Ante situaciones futuras considero que después de todas la experiencia vivida y aprendizajes obtenidos, de manera inicial realizaría una consulta o investigación (según sea el caso) o uno de la biblioteca Tuya o de la intranet para entender con mayor profundidad la temática, estrategia o ejercicio que se desea aplicar y posterior a ello, asesorarse con expertos en el campo para mayor exactitud en los resultados de este, presentando y realizando las respectivas mejoras al entregable.

Finalmente, durante mi estancia en la organización tuve un aprendizaje constante, puesto que, a medida que se iban desarrollando los temas, actividades y ejercicios fui adquiriendo un conocimiento y dominio con la ayuda de personas expertas y capacitadas en esos ámbitos. De igual forma, las actividades con respecto a la cultura de la seguridad, se podrían considerar como aquella en la que se tuvo mayor aprendizaje, debido a que, para su realización se debe tener presente y claro los términos (phishing, Bec y semejantes), las buenas prácticas para prevenirlo y ejercicios, charlas y actividades que concientizan a los miembros de Tuya S.A ante posibles riesgos.

5. Recomendaciones.

5.1 Para lo estratégico y/o lo operativo

Teniendo en consideración el proceso realizado en la compañía de financiamiento Tuya S.A en donde se incluye los aprendizajes, anécdotas y experiencias a nivel área y compañía considero que, una de las propuestas a tener en cuenta la organización debe ser encaminada a la asignación del líderes de los diferentes equipos de la organización y que a pesar de sus conocimientos, no son claros, oportunos y congruentes con los requerimientos solicitados puesto que, este debe ir en concordancia con el proceso, ejercicios e implementación de cada una de las actividades, ejercicios y estrategias que presenta el equipo, entendiendo la finalidad, sin generar juicios de valor o propuestas ajenas a las metas u objetivos que se esperan generar.

Además de lo anterior, la organización debería ampliar sus equipos de trabajo en las áreas donde la capacidad de trabajo es superior a la capacidad humana, debido a que, se puede generar una sobrecarga laboral por incremento en las actividades y disminución del personal, retrasando la entrega de las actividades, priorización o recorte de entregables.

Otra propuesta sería que, a pesar de que la compañía opere bajo el modelo de agilismo, la organización debe tener mayor control y realizar de una manera pasiva los ajuste, ya sea de equipos en relación con cambios de áreas, modificación de nombres, asignaciones y cargos de liderazgo, ya que esto modifica de una manera brusca las operaciones y la recopilación de información en relación a los diferentes reportes y búsquedas de la misma.

De igual manera, en cuanto a la capacidad de los equipos de trabajo, los líderes de los COE superiores deben tener en cuenta las codificaciones que se realizan en cada Q de acuerdo a las actividades y objetivos planteados para el año; por ello, no

deben modificar sin previo aviso o a convicción de ellos la ruta de trabajo del equipo, generando con esto problemas de planeación y modificación de los tiempos de entrega cumplimientos de objetivos propuestos.

Finalmente, la comunicación en Tuya S.A. debe ser una de las propuestas a resaltar puesto que, en algunas ocasiones en compleja la interacción con algunos líderes o diferentes personas de la organización ya sea por la agenda u ocupación que esta persona tenga, lo que genera que en algunas casos se tenga que solicitar con ayuda del líder o a través de un llamado de atención por parte del superior con el fin de tener alguna respuesta, generando impedimentos en la realización de las actividades que tenga relación con ellos como lo es el inventario de activos, modelado de roles y algunas actividades de cultura.

5.2 Para las prácticas

Como practicante del área de seguridad de la información a manera de propuesta de mejora propongo al equipo de trabajo, continuar con su proceso de acompañamiento y acogida a nuevos miembros, permitiendo así, una realización de manera amena la práctica profesional y las funciones que en esta se requieren, permitiendo una continua comunicación en el asesoramiento y acompañamiento en su proceso de inducción y adaptación, haciéndolo partícipe y protagonista de las estrategias y actividades que en este realizan, brindando la confianza para relacionarse, aprender y disfrutar su tiempo de práctica igual o mejor al vivido por mí en el periodo de práctica 2022-2. Así mismo, considero esto como un aspecto positivo y que se debe seguir en el tiempo.

En relación con las actividades propuestas por el equipo, recomiendo una realización de acercamiento de manera consecutiva para permitir al empleado y equipo de trabajo realizar pausas activas a modo de formaciones, capacitaciones, etc., para salir de la rutina laboral y generar un mayor acercamiento entre los miembros del equipo.

Para la modalidad de trabajo virtual que se realiza en el COE de seguridad de la información, recomiendo que se siga trabajando en alternativas de comunicación, permitiendo de esta manera un asesoramiento, acompañamiento y solución de inquietudes de manera ágil y eficiente. De igual forma, el equipo presenta una gran familiaridad con esta modalidad, lo que, ha permitido confianza y familiaridad con cada uno de ellos, por este, esto se debe ser trabajando un mejorando en el pasar del tiempo.

Al realizar las diferentes charlas y reuniones con diferentes miembros de la organización, recomiendo al equipo realizar sesiones con expertos o personas enfocadas en el tema de oratoria y manejo del escenario para pánico escénico o mejor la interpretación a la hora de interactuar con el público o compartir la información.

Finalmente, se recomienda generar mayores espacios para las sesiones de cultura y conocimiento de la ciberseguridad, lo que permite un mayor aprendizaje y manejo de los temas expuestos en las diferentes alternativas de trabajo (pruebas, ejercicios, simulacros, etc.) existentes en este equipo, permitiendo conocer, actualizar y evolucionar en relación con nuevos temas para conocer de manera constante en los cambios existentes en seguridad, ataques, prevención y cuidado de la información.

6. Referencias

- Analitik, V. (2022). Tarjeta de crédito para comerciantes quiere conquistar varias ciudades de Colombia. Valora Analitik. https://www.valoraanalitik.com/2022/03/05/tarjeta-de-credito-para-comerciantes-quiere-conquistar-en-varias-ciudades/

- Arteaga, N. (2015). *Con compra de 50% de Tuya, el Grupo Éxito llega al sector financiero*. La República. https://www.larepublica.co/empresas/con-compra-de-50-de-tuya-el-grupo-exito-llega-al-sector-financiero-2271936

- Belcic, I. (2020). *Guía esencial del phishing: Cómo funciona y cómo defenderse*. Avast. https://www.avast.com/es-es/c-phishing#topic-1

- Centro Cibernético Policial. (s. f.). B.E.C *(Business Email Compromise)*. Policía nacional de Colombia.https://caivirtual.policia.gov.co/sites/default/files/darc_b.e.c._business_email_compromise.pdf

- El Colombiano (2022). *¡No caiga en la trampa! Son falsos los correos para desbloquear la tarjeta 'Tuya' del Éxito.* El colombiano. https://www.elcolombiano.com/antioquia/correos-para-desbloquear-la-tarjeta-tuya-de-exito-son-falsos-FK19022575

- Gallardo, Y. & Moreno, A. (1999). *Recolección de información*. ICFES. https://academia.utp.edu.co/grupobasicoclinicayaplicadas/files/2013/06/3.-Recolecci%C3%B3n-de-la-Informaci%C3%B3n-APRENDER-A-INVESTIGAR-ICFES.pdf

- La Fábrica de Pensamiento instituto de Auditores Internos de España (2013). *Definición e implantación de Apetito de Riesgo*. Fundación Mapfre. https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

- La República S.A.S. (2022). *Tuya y Bancolombia siguen siendo los líderes en tarjetas de crédito durante este año*. Diario La República. https://www.larepublica.co/finanzas/los-lideres-en-tarjetas-de-credito-vigentes-se-mantienen-siendo-tuya-y-bancolombia-3432529

- Mera. L, Baque, L & Herrera, M. (2019). *Evaluación del nivel de madurez como función de la gestión de activos*. Revista De Estudios Empresariales. Segunda edición, (2), 177–189. https://revistaselectronicas.ujaen.es/index.php/REE/article/view/3741

- National Institute of Standards and Technology. (s.f). *Qué es y cómo funciona el Marco de Ciberseguridad NIST*. https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf

- Núñez. E, (2011). *Gestión tecnológica en la empresa: definición de sus objetivos fundamentales.* Revista de Ciencias Sociales, Vol. XVII. https://www.redalyc.org/articulo.oa?id=28022755013

- Palacio. C, (2021). *Gestión de estrategias de seguridad de la información.* SharePoint. Documento de la empresa.

- Semana. (2022). Falabella, Tuya y Banco de Bogotá lideran ranking con más tarjetas de crédito bloqueadas en 2022. Semana. https://www.semana.com/finanzas/credito/articulo/falabella-tuya-y-banco-de-bogota-lideran-ranking-con-mas-tarjetas-de-credito-bloqueadas-en-2022/202226/

- Tuya. (2021). *Composición accionaria*. Tuya. https://www.tuya.com.co/sites/default/files/2021-01/COMPOSICI%C3%93N%20ACCIONARIA%20enero%202021.pdf

- Tuya. (2022a). *Nuestra compañía*. Tuya S.A. https://www.tuya.com.co/nuestra-compania

- Tuya. (2022b). *Trabaje con nosotros*. Tuya S.A. https://trabajeconnosotros.tuya.com.co/

- Tuya. (s. f.). *Sistema de administración de riesgos*. Tuya S.A. https://www.tuya.com.co/sites/default/files/2018-10/Sistema%20de%20Administracion%20de%20Riesgos.pdf

- Unidad Administrativa Especial del Estado. (2016). *Guía de inventario de activos, clasificación y publicación de información.* Agencia nacional de defensa jurídica del estado. https://www.defensajuridica.gov.co/servicios-al-

ciudadano/ley_transparencia/Documents/guia_inventario_activos_clasificacion_publicacion_de_informacion_130916.pdf

- Ventura, M. (2021). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020*. Universidad Privada del Norte. https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2c%20Mishell%20Alisson.pdf?sequence=11&isAllowed=y

- Vega, E. (2021). *Seguridad de la información.* ÁREA DE INNOVACIÓN Y DESARROLLO, S.L. https://www.3ciencias.com/libros/libro/seguridad-de-la-informacion/

- Vesga, D. (2022). *Tuya y Bancolombia siguen siendo los líderes en tarjetas de crédito durante este año*. La República. https://www.larepublica.co/finanzas/los-lideres-en-tarjetas-de-credito-vigentes-se-mantienen-siendo-tuya-y-bancolombia-3432529